# UTILITY PATENT APPLICATION TRANSMITTAL

*(Only for new nonprovisional applications under 37 CFR 1.53(b))*

| | |
|---|---|
| *Attorney Docket No.* | 862.C2012 |
| *First Named Inventor or Application Identifier* | |
| YOSHIJI KANAMOTO | |
| *Express Mail Label No.* | |

## APPLICATION ELEMENTS

*See MPEP chapter 600 concerning utility patent application contents.*

**ADDRESS TO:** Commissioner for Patents, Box Patent Application, Washington, DC 20231

1. [X] Fee Transmittal Form (Submit an original, and a duplicate for fee processing)
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [X] Specification — *Total Pages* 46
4. [X] Drawing(s) *(35 USC 113)* — *Total Sheets* 7
5. [X] Oath or Declaration — *Total Pages* 1
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 17 completed)* ***[Note Box 6 below]***
      i [ ] DELETION OF INVENTOR(S) Signed Statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [X] Application Data Sheet. See 37 CFR 1.76
7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. [ ] Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] paper
   c. [ ] Statements verifying identity of above copies

### ACCOMPANYING APPLICATION PARTS

9. [X] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [ ] Power of Attorney
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [ ] Preliminary Amendment
14. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Other. _____

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No. __/_____

*Prior application information:* *Examiner* _____ *Group/Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

### 18. CORRESPONDENCE ADDRESS

[X] Customer Number or Bar Code Label — 05514 (Insert Customer No. or ~~Attach bar code label here~~) — or [ ] Correspondence address below

| | | | | | |
|---|---|---|---|---|---|
| NAME | | | | | |
| Address | | | | | |
| City | | State | | Zip Code | |
| Country | | Telephone | | Fax | |

| CLAIMS | (1) FOR | (2) NUMBER FILED | (3) NUMBER EXTRA | (4) RATE | (5) CALCULATIONS |
|---|---|---|---|---|---|
| | TOTAL CLAIMS (37 CFR 1.16(c)) | 33-20 = | 13 | X $ 18.00 = | $ 234.00 |
| | INDEPENDENT CLAIMS (37 CFR 1.16(b)) | 3-3 = | 0 | X $ 78.00 = | $ 0.00 |
| | MULTIPLE DEPENDENT CLAIMS (if applicable) (37 CFR 1.16(d)) | | | $260.00 = | $ 0.00 |
| | | | | BASIC FEE (37 CFR 1.16(a)) | $ 690.00 |
| | | | Total of above Calculations = | | $ 924.00 |
| | Reduction by 50% for filing by small entity (Note 37 CFR 1.9, 1.27, 1.28). | | | | |
| | | | | TOTAL = | $ 924.00 |

19. Small entity status

a. ☐ A small entity statement is enclosed

b. ☐ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.

c. ☐ Is no longer claimed.

20. ☒ A check in the amount of $ 924.00 to cover the filing fee is enclosed.

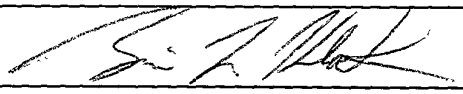
21. ☒ A check in the amount of $ 40.00 to cover the recordal fee is enclosed.

22. The Commissioner is hereby authorized to credit overpayments or charge the following fees to Deposit Account No. 06-1205:

a. ☒ Fees required under 37 CFR 1.16.

b. ☐ Fees required under 37 CFR 1.17.

c. ☐ Fees required under 37 CFR 1.18.

| *SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED* | |
|---|---|
| NAME | Brian L. Klock - Reg. No. 36,570 |
| SIGNATURE |  |
| DATE | September 29, 2000 |

BLK\cmv

INVENTOR INFORMATION

Inventor One Given Name: Yoshiji
Family Name: KANAMOTO
Postal Address Line One: c/o Canon Daini Moegino Ryo
Postal Address Line Two: 27-6, Moegino, Aoba-ku
City of Residence: Yokohama-shi
State or Province of Residence: Kanagawa-ken
Country of Residence: Japan
Citizenship Country: Japan

CORRESPONDENCE INFORMATION

Correspondence Customer Number: 05514
Fax: (212) 218-2200

APPLICATION INFORMATION

Title Line One: INFORMATION PROCESSING METHOD AND APPARATUS

Total Drawing Sheets: 7
Formal Drawings?: Yes
Application Type: Utility
Docket Number: 862.C2012
Secrecy Order in Parent Appl.?: No

REPRESENTATIVE INFORMATION

Representative Customer Number: 5514

PRIOR FOREIGN APPLICATIONS

Foreign Application One: 11-279374
Filing Date: 09-30-1999
Country: JAPAN
Priority Claimed: Yes

SPECIFICATION

TITLE OF THE INVENTION

# INFORMATION PROCESSING METHOD AND APPARATUS

## FIELD OF THE INVENTION

The present invention relates to information processing method and apparatus, and more particularly, to information processing method and apparatus for prevention against original image reproduction from image data.

## BACKGROUND OF THE INVENTION

Generally, when image information is stored into a memory, gray scale levels of respective pixels are obtained as numerical values and the data is stored in a predetermined order in continuous memory areas.

Further, the data string format upon storage of pixel information into memory differs in accordance with format or implementation of data processing algorithm of device to input images to a frame memory or device to output images from the memory, however, memory access is always made in accordance with the same procedure inside the device.

That is, when pixel information stored in a

particular address is accessed, the same address value is always used.

Accordingly, in an image processing apparatus having a conventional storage device, there is a strong linkage between the content of the frame memory and an original image. In this case, if the content of the frame memory can be obtained or referred to by any means, the original image can be comparatively easily reproduced even though the procedure upon image data generation is not known.

However, this fact is very inconvenient in consideration of image information security.

For example, when the content of frame memory is stored in a file in another place or transferred to another place via a network, a third person may have an opportunity to access the image data during such data transfer which is often performed as daily work. As a result, there is a high probability that the image data is reproduced and the content of the original image is known.

Generally, confidential documents and the like are encrypted for protection of the contents. However, encryption is generally complicated and time-consuming processing, and further, installation of the encryption processing program is often difficult.

## SUMMARY OF THE INVENTION

The present invention has been made in consideration of the above situation, and has its object to provide information processing method and apparatus to realize a function to cause difficulty in analysis of data, even if the data is read by a third person, by a particular memory addressing method.

Another object of the present invention is to provide information processing method and apparatus which realize a function to, especially upon image data storage, weaken the linkage between a frame memory and an original image by the particular memory addressing method, so as to cause difficulty in reproduction of the original image.

According to the present invention, to solve the above objects, provided is an information processing apparatus for storing data into storage means, comprising: key input means for inputting a desired key code; address conversion means for converting a first address designating a storage position of the storage means for holding the data to a second address based on the desired key code inputted by the input means; and

storage control means for storing the data in a storage area of the storage means designated by the second address obtained by the address conversion means.

In the information processing, the address conversion means performs mutually reversible conversion between the first address and the second address by the same key code. Further, the address conversion means interchanges several address lines of the first address based on the desired key code inputted by the key input means to generate the second address. Further, if the data is image data, the address conversion means performs address conversion so as to interchange positions of a predetermined areas divided from the image.

Further, the information processing apparatus further comprises key code conversion means for generating a second key code from the input desired key code, and the address conversion means converts the first address to the second address based on the second key code.

Further, The information processing apparatus further comprises input selection means for selecting one input destination from plural data input destinations, and data from the input destination selected by the input selection means is stored into the storage means.

Further, in the information processing apparatus, the plural data input destinations include a scanner, a large-capacity storage device and a communication device.

Further, the information processing apparatus further comprises output selection means for selecting one output destination from plural data output destinations, and data read from the storage means is outputted to the output destination selected by the output selection means.

Further, in the information processing apparatus, the plural data output destinations include a printer, a large-capacity storage device, a display and a communication device. Further, the data is image data.

Further, the information processing apparatus further comprises a scanner for inputting data to be stored in the storage means and a printer for outputting data stored in the storage means, and the information processing apparatus operates as a copying machine. Further, in the information processing apparatus a scanner or communication device can be selected as an input source for inputting data to be stored in the storage means, and the communication device and a printer can be selected as an output destination for outputting data from the storage means, further, the information processing apparatus operates as a facsimile machine.

Further, the information processing apparatus further comprises address conversion designation means for designating execution or non-execution of address

conversion by the address conversion means.

Further, provided is a data security method for the information processing apparatus, comprising the steps of: for encryption, storing input data into the storage means while converting an address by the address conversion means based on the desired key code inputted from the key input means, and outputting the data as encrypted data to the outside and holding the data; and for decryption, storing the held data as input data into the storage means while converting the address by the address conversion means based on the same key code as the desired key code inputted from the key input means, and outputting the data as decrypted data to the outside.

Further, provided is a data security method for the information processing apparatus, comprising the steps of: for encryption, storing the key code and input data into the storage means while converting an address by the address conversion means based on the desired key code inputted from the key input means, and outputting them as encrypted data to the outside and holding the data; and for decryption, storing the held data as input data into the storage means while converting the address by the address conversion means based on the same key code as the desired key code reproduced from the held data, and outputting the data as decrypted data to the outside.

Further, provided is an information processing for storing data into storage means, comprising: a key input step of inputting a desired key code; an address conversion step of converting a first address designating a storage position of the storage means for holding the data to a second address based on the desired key code inputted at the input step; and a storage control step of storing the data in a storage area of the storage means designated by the second address obtained at the address conversion step.

In the information processing method, at the address conversion step, mutually reversible conversion is performed between the first address and the second address by the same key code. Further, at the address conversion step, several bits of the first address are interchanged based on the desired key code inputted at the key input step, to generate the second address. Further, at the address conversion step, if the data is image data, address conversion is performed so as to interchange positions of a predetermined areas divided from the image.

Further, the information processing method further comprises a key code conversion step of generating a second key code from the input desired key code, and at the address conversion step, the first address is converted to the second address based on the second key

code. Further, the data is image data.

Further, provided is a security method in use of the information processing method in a printer, comprising the steps of: encrypting received image data by the information processing method and print-outputting the data; and reading the print-outputted encrypted data by a scanner or copying machine capable of decryption in accordance with the same key as that used in encryption by the information processing method.

Further, provided is a security method in use of the information processing method in a scanner, comprising the steps of: encrypting read image data by the information processing method; and print-outputting or decoding the encrypted data by a printer or computer capable of decryption in accordance with the same key as that used in encryption by the information processing method.

Further, provided is a security method in use of the information processing method in a copying machine, comprising the steps of: encrypting read image data by the information processing method and print-outputting the data; and reading the print-outputted encrypted data in accordance with the same key as that used in encryption by the information processing method.

Further, provided is a security method in use of the information processing method in a facsimile machine,

comprising the steps of: encrypting read image data by the information processing method and transmitting the data; and decrypting the received encrypted data in accordance with the same key as that used in encryption by the information processing method and print-outputting the data.

Further, the security method further comprises the steps of: print-outputting the received encrypted data; and reading the print-outputted encrypted data, decrypting the data in accordance with the same key as that used in encryption by the information processing method and print-outputting the data.

Further, provided is a security method in use of the information processing method in a communication device, comprising the steps of: encrypting data by the information processing method and transmitting the data; and decrypting the received encrypted data in accordance with the same key as that used in encryption by the information processing method and print-outputting the data. Further, the key is embedded in an encryption key to be transmitted.

Further, provided is a security method in use of the information processing method in a computer, comprising the steps of: encrypting data by the information processing method and storing the data; and decrypting the stored encrypted data in accordance with

the same key as that used in encryption by the information processing.

Further, provided is a storage medium for storing an information processing program in case of storing data into storage means in a computer-readable format, wherein the information processing program includes at least an address conversion step of converting a first address designating a storage position of the storage means for storing the data into a second address based on an input desired key code.

Further, in the storage medium, the information processing program further includes: a key input step of inputting a desired key code; and a storage control step of storing the data into a storage area of the storage means designated by the second address obtained at the address conversion step. Further, at the address conversion step, mutually reversible conversion is performed between the first address and the second address by the same key code. Further, at the address conversion step, wherein at the address conversion step, several bits of the first address are interchanged based on the desired key code inputted at the key input step, to generate the second address.

Other features and advantages of the present invention will be apparent from the following description taken in conjunction with the accompanying

drawings, in which like reference characters designate the same name or similar parts throughout the figures thereof.

## BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.

Fig. 1 is a block diagram showing the basic construction of an information processing apparatus according to a first embodiment of the present invention;

Fig. 2 is a flowchart showing processing for storing image data into a frame memory of the information processing apparatus according to the first embodiment;

Fig. 3 is a flowchart showing processing for reading image data from the frame memory of the information processing apparatus according to the first embodiment;

Fig. 4 is a block diagram showing in detail an address conversion unit of the first embodiment;

Fig. 5 is a block diagram showing the basic

construction of the information processing apparatus according to a second embodiment of the present invention;

Fig. 6 is a flowchart showing processing for reading image data from the frame memory of the information processing apparatus according to the second embodiment; and

Fig. 7 is a block diagram showing the basic construction of the information processing apparatus according to a third embodiment of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the present invention will now be described in detail in accordance with the accompanying drawings.

<First Embodiment>

Fig. 1 is a block diagram showing the construction of an information processing apparatus to which a first embodiment of the present invention is applied.

The information processing apparatus of the embodiment has a function to scan an original document and store image data into a large-capacity storage device, and a function to search the large-capacity storage device for a target document and print-output the document from an output device such as a printer, in

accordance with necessity.

In Fig. 1, a frame memory 1 stores image data which is an object of processing.

An image input selector 2 designates a device as an input source of image data to be inputted into the frame memory 1 such as an image scanner 2000 or a large-capacity storage device 1000. A communication device may be included in the input sources.

Further, an image output selector 8 designates an output destination for image data read out of the frame memory 1, such as a printer 1001, the large-capacity storage device 1000 or a display monitor 1002. The communication device may be included in the output destination devices.

An address converter 3, as an element characteristic of the present embodiment, converts a physical address to designate a data storage position on the frame memory 1. The address converter 3 has an operation unit 4, a key register 5 and an address conversion unit 6.

The operation unit 4 is a data input device having a keyboard, a pointing device and the like.

The operation unit 4 accepts input of numeral as a conversion key referred to by the address conversion unit 6, from an operator. The input numeral, which is information as a key to generate address conversion

pattern to be described later, plays a role of encryption key according to the present embodiment. Further, mode designation data designating a normal mode to access the frame memory 1 without address conversion or an encryption mode to access the frame memory 1 with address conversion is inputted. The input numeral (encryption key) and the mode designation data are stored into the key register 5. Further, an address to access the frame memory 1 or a designation address designating an address range may be inputted.

Note that when the entire address range of the frame memory 1 is to be converted, the designation address is not necessary. The mode designation data and the numeral (encryption key) are transferred to the address conversion unit 6. The address conversion unit 6 performs processing in accordance with these data. Further, when the designation address is inputted, it is sent to an address output unit 7. The address output unit 7 outputs an address to the address conversion unit 6 based on the designation address to designate the address or address range. The address to access the frame memory or designation address designating address range may be inputted into the address output unit 7 from an image input unit or other external memory controller than the operation unit 4.

When image data inputted via the image input

selector 2 is stored into the frame memory 1, if the mode designation data designating the normal mode is inputted from the key register 5, the address conversion unit 6 outputs an address to the frame memory 1 based on the physical address generated by the address output unit 7. In synchronization with the address output, the predetermined image data is provided to the frame memory 1 via the image input selector 2, and the image data is stored.

On the other hand, if the encryption mode is designated, the address conversion unit 6 performs conversion on the physical address provided from the address output unit 7 by using the numeral stored in the key register 5. Then, the address conversion unit 6 outputs the converted address to the frame memory 1. In synchronization with the address output, the predetermined image data is provided to the frame memory 1 via the image input selector 2, and the image data is stored.

Accordingly, from hardware of an external device which accesses the frame memory 1, it appears that the data is written into the frame memory 1 in a position corresponding to the physical address generated by the address output unit 7. However, the position in which the data is actually written differs in accordance with key.

The address conversion mentioned above can be carried out by using a conversion table which can converts each address of the frame memory 1 into another one, randomly and biunivoquely. The conversion process is performed as follows, when the address and the key are provided, the address conversion unit 6 adds the address and the key, and inputs the result of addition into the conversion table, then a converted address is obtained as an output from the conversion table, wherein if the sum of the address and the key is greater than the maximum value of addresses of the frame memory 1, a value generated by subtracting the maximum value from the sum is provided to the conversion table.

By the above processing, the image data can be stored into the frame memory 1 in a manner such that even if the image data in the frame memory 1 is read from the outside, original image reproduction cannot be made from the stored image data.

Next, when image data stored in the frame memory 1 is to be read, the address output unit 7 generates a read address and outputs it to the address conversion unit 6. If the normal mode is designated, the address conversion unit 6 supplies the same address as that inputted from the address output unit 7 to the frame memory 1, and data in a position corresponding to the address is outputted from the frame memory 1 to the

image output selector 8.

As described above, if the encryption mode is designated, the address conversion unit 6 converts the physical address provided from the address output unit 7 by using the numeral stored in the key register 5. Then the address conversion unit 6 outputs the converted address to the frame memory 1. In synchronization with the address output, the image data stored in the input address is read out and outputted to the image output selector 8. The address conversion for image reading can be carried out by an invert conversion of the conversion for image storing. That is the provided address is converted to an address by referring the conversion table in a reverse way, the address for reading is obtained by subtracting the key from the output of the conversion table, wherein if the output is smaller than key, a value generated by adding the maximum value of addresses of the frame memory 1 to the subtraction is provided as the address for reading to the frame memory 1.

The image output selector 8 outputs the input image data to, e.g., the large-capacity storage device 1000. The large-capacity storage device 1000 holds the data.

If the image data stored in the large-capacity storage device 1000 is printed out from the printer 1000,

for example, the image input selector 2 selects the large-capacity storage device 1000 as an image data input destination, and the image output selector 8 selects the printer 1001 as an output destination.

To normally read image data from the frame memory 1, the above-described key inputted from the operation unit 4 or external device is necessary.

That is, when the image data is read from the frame memory 1, if a wrong key is inputted, image data for normal reproduction of original image cannot be outputted from the frame memory 1. Thus, the original image reproduction from image data stored in the frame memory 1 can be protected.

Next, the flowchart of Fig. 2 shows a processing operation for storing image data into the frame memory 1 according to the present embodiment.

In Fig. 2, at step S1, the operation unit 4 inputs mode designation data designating the normal mode or the encryption mode.

At step S2, the operation unit 4 checks the input mode. If the input mode is the normal mode, as it is not necessary to perform address conversion, the process proceeds to step S10, while if the input mode is the encryption mode, proceeds to step S3.

At step S3, the operation unit 4 inputs an encryption key as a cipher, and stores it into the key

register 5. The encryption key is not necessarily a numeral but may be an arbitrary alphabet string or the like. However, in consideration of normal stand-alone business machines, as it is convenient to limit ten-keys as means for inputting the key, only numerals are inputted in this embodiment. Next, if necessary, the operation unit 4 inputs a write designation address or address designating a write section with respect to the frame memory 1, and transmits the address to the address output unit 7. Note that if the entire area of the frame memory is to be subjected to writing processing, the input of designation address or writing section is not necessary.

At step S4, the address conversion unit 6 inputs the encryption key from the key register 5, then converts an address outputted from the address output unit 7 based on the encryption key, and supplies the converted address to the frame memory 1.

In the encryption-key based address conversion, the address space before the conversion and that after the conversion must be in one-to-one correspondence. If only this condition is satisfied, any method of encryption-key based address conversion is used. More specifically, the address conversion may be performed by using a function performing one-to-one mapping with regard to each element of the address space of the frame

memory, or by address bit exchange by referring to a conversion table holding address bit exchange rules based on encryption key.

On the other hand, at step S10, as the normal mode is designated, the address conversion unit 6 outputs the address inputted from the address output unit 7 to the frame memory 1 without any conversion. Note that if the address output unit 7 is included in an external device, step S10 may be omitted.

At step S5, in the frame memory 1, in synchronization with the address input from the address conversion unit 6, image data sent from the image input selector 2 is stored into an internal cell of the address.

At step S6, if there is next address input from the address output unit 7, the process proceeds to step S7, while if there is no address input, the process ends.

At step S7, if the current mode is the encryption mode, the process returns to step S4 to repeat the processing by the address conversion unit 6. If the current mode is the normal mode, the process returns to step S10 to repeat the processing by the address conversion unit 6.

Note that when image data in the encryption mode is written into the frame memory, a predetermined tag code indicating that the writing has been made in the

encryption mode may be written, with linkage to a pair of head address and end address before conversion, into a predetermined field of the frame memory. By using the tag code, it can be determined later whether corresponding image data has been stored in the encryption mode or not by designating the head address before conversion and referring to the field.

Further, in the above example, the step of address conversion (S4) and the step of not performing address conversion (S10) are provided. However, it may be arranged such that in case of the encryption mode, an address conversion table is generated based on an encryption key, while in case of the normal mode, address conversion is not performed. In this arrangement, the processing in Fig. 2 can be more simplified.

Next, a processing procedure for reading image data from the frame memory 1 will be described with reference to the flowchart of Fig. 3.

In Fig. 3, at step S11, mode designation data designating the normal mode or the encryption mode is inputted from the operation unit 4.

At step S12, the operation unit 4 checks the input mode. If the mode is the normal mode, as address conversion is not necessary, the process proceeds to step S20, while if the mode is the encryption mode, the process proceeds to step S13. Note that if the entire

address range of the frame memory area is to be converted, the input of designation address or section is not necessary.

At step S13, an encryption key is inputted from the operation unit 4, and the encryption key is stored into the key register 5. Further, a read out designation address or an address designating a read out section with respect to the frame memory 1 is inputted from the operation unit 4, and is transmitted to the address output unit 7.

At step S14, the encryption key is inputted from the key register 5 into the address conversion unit 6. Then an address outputted from the address output unit 7 is converted based on the encryption key, and is supplied to the frame memory 1.

On the other hand, at step S20, as the normal mode is designated, the address conversion unit 6 outputs the address inputted from the address output unit 7 to the frame memory 1 without any conversion.

At step S15, in the frame memory 1, in synchronization with the address input from the address conversion unit 6, image data is read out from an internal cell of the address and sent to the image output selector 8.

At step S16, if there is next input from the address output unit 7 into the address conversion unit 6,

the process proceeds to step S17, while if there is no input, the process ends.

At step S17, if the mode is the encryption mode, the process returns to step S14 to repeat the processing by the address conversion unit 6. If the mode is the normal mode, the process returns to step S20 to repeat the processing by the address conversion unit 6.

Note that in the reading processing in Fig. 3, the address designation may be performed from other external devices than the operation unit 4. In such case, step S10 may be omitted. Further, it may be arranged such that in case of the encryption mode, an address conversion table is generated based on an encryption key, while in case of the normal mode, address conversion is not performed. In this arrangement, the processing in Fig. 3 can be more simplified.

Next, the construction of the address conversion unit 6 will be described with reference to Fig. 4. Note that Fig. 4 also shows related processing units.

Referring to Fig. 4, the frame memory 1 has a 16 Mbyte capacity, where 1 byte is used for storing 256 level single-color data. For example, the frame memory 1 can hold raster-scanned 4096 × 4096 pixel image information.

Further, a 24-bit (8 bits × 3) code corresponding to an encryption key inputted from the operation unit 4

is inputted from the key register 5.

Further, a 24-bit frame address is inputted from the address output unit 7.

Note that the present invention is not limited to these numbers of bits.

A several digit decimal integer numerical value is inputted by a user from the operation unit 4, then the numerical value is converted into a hexadecimal number, and stored into the key register 5. From a bit string constructing the register, arbitrary 8 bits are extracted, and three patterns are generated. The generated respective 8-bit data are inputted and stored into respective tables 6a to 6c.

The data stored in the respective tables 6a to 6c are used as keys designating conversion patterns to the converters 6d to 6f.

The address conversion unit 6 performs address conversion in three steps.

The converter 6d performs conversion for 12 bits corresponding to the lower order address. At this time, the conversion processing may be performed in 1-pixel units, however, in actual image information, if address conversion is performed by greater block (n × n), reproduction of original image information is sufficiently difficult from the converted image information.

Accordingly, in this example, to simplify circuits around the converter, 16-pixel address conversion is performed by address-converting only higher order 8 bits without conversion of lower order 4 bits.

The address conversion by the converter 6d corresponds to interchanging 256 horizontal stripe areas (horizontally-continuous 16 pixel areas) in the horizontal direction, in the 4096 × 4096 pixel image information on the frame memory, in accordance with the content indicated by the table 6a.

On the other hand, the address conversion by the converter 6f corresponds to interchanging 256 vertical stripe areas (vertically-continuous 16 pixel areas) in the vertical direction in accordance with the table 6c.

The address conversion by the converter 6e corresponds to separating the image into 256 × 256 areas (vertically- and horizontally-continuous 16 pixel areas) and interchanging them in accordance with the table 6b.

As a result, these three address conversion make reproduction of original image information sufficiently difficult if image information stored in the frame memory 1 is read out by an address from the address output unit 7.

In Fig. 4, the tables and the converters are separately provided, however, as long as address conversion is made in accordance with key data, the

present invention is not limited to this arrangement. For example, to simplify the circuit construction, it is preferable to construct a look-up table by using a programmable logic array, to obtain a conversion address from the table, with 8-bit information from the key register 5 and address from the address output unit 7 as input. Further, to improve security, it is preferable to sequentially change the conversion method in the address conversion unit 6. Further, in such case it is preferable to realize the address conversion with software.

If address conversion is not performed, the input address from the address output unit 7 is selected by multiplexers 6h and 6g, and the higher order and lower order addresses in the frame memory 1a are respectively designated.

Thereafter, data is sequentially read out from the frame memory 1 from the head address, and stored in the large-capacity storage device 1000 or the like via the image output selector 8.

The encryption processing upon storage of image data into the large-capacity storage device 1000 or the like is as described above. Upon image reproduction, image information is temporarily stored into the frame memory 1 from the head address, then the data is read from the frame memory 1 by using an address converted by

the address conversion unit 6 as in the case of storage, outputted from the address output unit 7, and the image is reproduced based on the data.

In this case, the management of encryption key is important. If the algorithm for generating output bits from the address conversion unit 6 or key register 5 is unknown, the key may be included in encrypted image data. Preferably, the encryption key in this case is time-varying data such as processing time. However, there is a possibility that the above algorithm is analyzed. To prevent the analysis of the algorithm, it is necessary to frequently change the algorithm.

<Second Embodiment>

The second embodiment shows a processing procedure for writing image data into the frame memory 1 in a case where the above-described tag code indicating type of the mode is written in a predetermined field of the frame memory 1 with linkage to a pair of head address and end address before conversion.

Fig. 5 shows the construction of the information processing apparatus according to the second embodiment. Fig. 5 differs from Fig. 1 in that a path to output data read from the frame memory 1 to the operation unit 4 is added, but the other elements are identical to those in Fig. 1. Accordingly, the corresponding processing units

have the same reference numerals.

Next, a processing procedure for normally reading predetermined image from the frame memory according to the present embodiment will be described with reference to Fig. 6.

In Fig. 6, at step S61, the operation unit 4 inputs output head address and end address from the frame memory 1 and writes them into the key register 5.

At step S62, the operation unit 4 outputs an address of predetermined area holding tag information to the address output unit 7. Further, the mode designation data designating the normal mode is stored in the key register 5. The address output unit 7 outputs the address of predetermined area holding the tag information to the address conversion unit 6. As the mode designation data designating the normal mode is inputted from the key register 5, the address conversion unit 6 supplies the address inputted from the address output unit 7 to the frame memory 1 without any conversion. Then tag related information stored in the supplied address area is read from the frame memory 1 and sent to the operation unit 4. The operation unit 4 searches the tag related information sent from the frame memory 1 for tag data related to the output head address inputted at step S61, and obtains the type of the mode.

At step S63, the operation unit 4 determines the

type of the mode obtained at step S61. If the mode is the normal mode, as address conversion is not necessary, the process proceeds to step S70, while if the mode is the encryption mode, the process proceeds to step S64.

At step S64, an encryption key is inputted from the operation unit 4. Further, the operation unit 4 transmits a write designation address or write section designation address with respect to the frame memory 1 to the address output unit 7.

At step S65, the operation unit 4 stores the encryption key inputted at step S64 into the key register 5.

At step S66, the encryption key is inputted from the key register 5 into the address conversion unit 6. Then, an address outputted from the address output unit 7 is converted based on the encryption key, and the converted address is supplied to the frame memory 1.

On the other hand, at step S70, as the normal mode is designated, the address conversion unit 6 outputs the address inputted from the address output unit 7 to the frame memory 1 without any conversion.

At step S67, in synchronization with the address input from the address conversion unit 6, image data is read out from an internal cell of the address from the frame memory 1, and sent to the image output selector 8.

At step S68, if there is next address input from

the address output unit 7, the process proceeds to step S69, while if there is no address input, the process ends.

At step S69, if the mode is the encryption mode, the process returns to step S66, to repeat the processing. If the mode is the normal mode, the process returns to step S70 to repeat the processing.

The image-data read out (reproduction) processing procedure in the second embodiment is as described above.

Note that as in the case of the first embodiment, various changes may be made in the construction of the address conversion unit 6 and encryption key management.

<Third Embodiment>

Next, the third embodiment will be described. In the first embodiment as shown in Fig. 1, the information processing apparatus is used for address conversion upon image storage and image reproduction as an independent apparatus, however, the present invention is not limited to such purpose.

For example, if the information processing apparatus according to the present invention is applied to a frame memory of a copying machine, the copying machine has an encryption function.

Fig. 7 shows the construction of a copying machine having an encryption function.

In Fig. 7, in an image input unit 9, a shift correction device 9b performs positional correction on an image read from an input device (scanner) 9a for preventing positional shift of original document on a platen. Then the corrected image is stored into a frame memory 11.

Since the operations of address output unit 9c, address converter 10 and its internal modules are the same as those in Fig. 1, the explanation of the operations will be omitted.

Further, data writing to the frame memory 11 is made with respect to an area designated by an address converted in accordance with a similar procedure to that described above.

The content of the frame memory 11 is finally read sequentially from the head address, and is outputted from an output unit 12.

Generally, as the output unit of copying machine is a printer, a printed output can be obtained. As the printed output is encrypted in accordance with a key inputted by a user from an operation unit 10a, it is illegible. To reproduce the original image, the encrypted document is read again from the image input unit 9, and is outputted in a decryption mode in accordance with the same key as that in the encryption. As the method of generating a conversion address of the

frame memory upon encryption and decryption is the same as that in Fig. 4, the explanation of the method will be omitted. Further, as described above, the encryption key may be included in a printed output for decryption without input from the operation unit 10a.

Further, in use of facsimile machine, as long as the machine has a memory to hold several pages of transmission document, encryption upon transmission is possible by providing the frame memory of the information processing apparatus according to the present invention. In this case, the encrypted document may be decrypted by an operator's inputting a predetermined key upon printing of confidential document.

Further, the purpose of the present invention is not limited to the frame memory. For example, the invention can be applied to a method for accessing a memory constructing a main storage device of a general computer.

In this case, as an area holding secret information is accessed by using address conversion by a key, even if the area is accessed by a third person who does not know the key, the position of the information or normal order of information cannot be obtained. Thus data security can be improved.

Note that in the above construction of the information processing apparatus, the address conversion

unit 6 is realized by circuits, however, processing equivalent to the processing by the address conversion unit 6 can be realized by software program which is stored into a memory and executed by a predetermined CPU. The advantage of this case is as described above.

As described above, an information storage device having an encryption function can be realized by providing a memory constructing a frame memory for storing an original image, adding a register and a converter to an address designation device, and providing means for performing conversion processing on a physical address inputted into the address designation device by using the converter in accordance with a value stored in the register.

Further, as described above, the frame memory addressing method according to the present invention weakens the linkage between the frame memory and an original image, and even if data is read by a third person, causes difficulty in reproduction of original image.

The present invention can be applied to a system constituted by a plurality of devices (e.g., a host computer, an interface, a reader and a printer) or to an apparatus comprising a single device (e.g., a copy machine or a facsimile apparatus).

Further, the object of the present invention can be also achieved by providing a storage medium storing program code for performing the aforesaid processes to a system or an apparatus, reading the program code with a computer (e.g., CPU, MPU) of the system or apparatus from the storage medium, then executing the program.

In this case, the program code read from the storage medium realizes the functions according to the embodiments, and the storage medium storing the program code constitutes the invention.

Further, the storage medium, such as a floppy disk, a hard disk, an optical disk, a magneto-optical disk, CD-ROM, CD-R, a magnetic tape, a non-volatile type memory card, and ROM can be used for providing the program code.

Furthermore, besides aforesaid functions according to the above embodiments are realized by executing the program code which is read by a computer, the present invention includes a case where an OS (operating system) or the like working on the computer performs a part or entire processes in accordance with designations of the program code and realizes functions according to the above embodiments.

Furthermore, the present invention also includes a case where, after the program code read from the storage medium is written in a function expansion card which is

inserted into the computer or in a memory provided in a function expansion unit which is connected to the computer, CPU or the like contained in the function expansion card or unit performs a part or entire process in accordance with designations of the program code and realizes functions of the above embodiments.

In a case where the present invention is applied to the aforesaid storage medium, the storage medium stores program code corresponding to the flowcharts described in the embodiments.

The present invention is not limited to the above embodiments and various changes and modifications can be made within the spirit and scope of the present invention. Therefore, to appraise the public of the scope of the present invention, the following claims are made.

WHAT IS CLAIMED IS:

1. An information processing apparatus having a step of storing data into storage means, comprising:

key input means for inputting a desired key code;

address conversion means for converting a first address designating a storage position of said storage means for holding the data to a second address based on said desired key code inputted by said input means; and

storage control means for storing said data in a storage area of said storage means designated by said second address obtained by said address conversion means.

2. The information processing apparatus according to claim 1, wherein said address conversion means performs mutually reversible conversion between said first address and said second address by the same key code.

3. The information processing apparatus according to claim 2, wherein said address conversion means interchanges several address lines of said first address based on the desired key code inputted by said key input means to generate said second address.

4. The information processing apparatus according to claim 2, wherein if said data is image data, said address conversion means performs address conversion so

as to interchange positions of a predetermined areas divided from the image.

5. The information processing apparatus according to claim 2, further comprising key code conversion means for generating a second key code from said input desired key code,

wherein said address conversion means converts said first address to said second address based on said second key code.

6. The information processing apparatus according to claim 1, further comprising input selection means for selecting one input destination from plural data input destinations,

wherein data from the input destination selected by said input selection means is stored into said storage means.

7. The information processing apparatus according to claim 4, wherein said plural data input destinations include a scanner, a large-capacity storage device and a communication device.

8. The information processing apparatus according to claim 1, further comprising output selection means for

selecting one output destination from plural data output destinations,

wherein data read from said storage means is outputted to the output destination selected by said output selection means.

9. The information processing apparatus according to claim 6, wherein said plural data output destinations include a printer, a large-capacity storage device, a display and a communication device.

10. The information processing apparatus according to claim 1, wherein said data is image data.

11. The information processing apparatus according to claim 1, further comprising a scanner for inputting data to be stored in said storage means and a printer for outputting data stored in said storage means,

wherein said information processing apparatus operates as a copying machine.

12. The information processing apparatus according to claim 1, wherein a scanner or communication device can be selected as an input source for inputting data to be stored in said storage means, and wherein said communication device and a printer can be selected as an

output destination for outputting data from said storage means, further wherein said information processing apparatus operates as a facsimile machine.

13. The information processing apparatus according to claim 1, further comprising address conversion designation means for designating execution or non-execution of address conversion by said address conversion means.

14. A data security method for the information processing apparatus in claim 1, comprising the steps of:

for encryption, storing input data into said storage means while converting an address by said address conversion means based on the desired key code inputted from said key input means, and outputting the data as encrypted data to the outside and holding the data; and

for decryption, storing said held data as input data into said storage means while converting the address by said address conversion means based on the same key code as said desired key code inputted from said key input means, and outputting the data as decrypted data to the outside.

15. A data security method for the information processing apparatus in claim 1, comprising the steps of:

for encryption, storing said key code and input data into said storage means while converting an address by said address conversion means based on the desired key code inputted from said key input means, and outputting them as encrypted data to the outside and holding the data; and

for decryption, storing said held data as input data into said storage means while converting the address by said address conversion means based on the same key code as said desired key code reproduced from said held data, and outputting said data as decrypted data to the outside.

16. An information processing method for storing data into storage means, comprising:

a key input step of inputting a desired key code;

an address conversion step of converting a first address designating a storage position of said storage means for holding the data to a second address based on said desired key code inputted at said input step; and

a storage control step of storing said data in a storage area of said storage means designated by said second address obtained at said address conversion step.

17. The information processing method according to claim 16, wherein at said address conversion step, mutually reversible conversion is performed between said first address and said second address by the same key code.

18. The information processing method according to claim 16, wherein at said address conversion step, several bits of said first address are interchanged based on the desired key code inputted at said key input step, to generate said second address.

19. The information processing method according to claim 17, wherein at said address conversion step, if said data is image data, address conversion is performed so as to interchange positions of a predetermined areas divided from the image.

20. The information processing method according to claim 17, further comprising a key code conversion step of generating a second key code from said input desired key code,

wherein at said address conversion step, said first address is converted to said second address based on said second key code.

21. The information processing method according to claim 16, wherein said data is image data.

22. A security method in use of the information processing method in claim 16 in a printer, comprising the steps of:

encrypting received image data by said information processing method and print-outputting the data; and

reading the print-outputted encrypted data by a scanner or copying machine capable of decryption in accordance with the same key as that used in encryption by said information processing method.

23. A security method in use of the information processing method in claim 16 in a scanner, comprising the steps of:

encrypting read image data by said information processing method; and

print-outputting or decoding the encrypted data by a printer or computer capable of decryption in accordance with the same key as that used in encryption by said information processing method.

24. A security method in use of the information processing method in claim 16 in a copying machine,

comprising the steps of:

encrypting read image data by said information processing method and print-outputting the data; and

reading the print-outputted encrypted data in accordance with the same key as that used in encryption by said information processing method.

25. A security method in use of the information processing method in claim 16 in a facsimile machine, comprising the steps of:

encrypting read image data by said information processing method and transmitting the data; and

decrypting the received encrypted data in accordance with the same key as that used in encryption by said information processing method and print-outputting the data.

26. The security method according to claim 25, further comprising the steps of:

print-outputting the received encrypted data; and

reading the print-outputted encrypted data, decrypting the data in accordance with the same key as that used in encryption by said information processing method and print-outputting the data.

27. A security method in use of the information

processing method in claim 16 in a communication device, comprising the steps of:

encrypting data by said information processing method and transmitting the data; and

decrypting the received encrypted data in accordance with the same key as that used in encryption by said information processing method and print-outputting the data.

28. The security method according to claim 27, wherein said key is embedded in an encryption key to be transmitted.

29. A security method in use of the information processing method in claim 16 in a computer, comprising the steps of:

encrypting data by said information processing method and storing the data; and

decrypting the stored encrypted data in accordance with the same key as that used in encryption by said information processing.

30. A storage medium for storing an information processing program in case of storing data into storage means in a computer-readable format,

wherein said information processing program

includes at least an address conversion step of converting a first address designating a storage position of said storage means for storing said data into a second address based on an input desired key code.

31. The storage medium according to claim 30, wherein said information processing program further includes:

a key input step of inputting a desired key code; and

a storage control step of storing said data into a storage area of said storage means designated by the second address obtained at said address conversion step.

32. The storage medium according to claim 30, wherein at said address conversion step, mutually reversible conversion is performed between said first address and said second address by the same key code.

33. The storage medium according to claim 30, wherein at said address conversion step, wherein at said address conversion step, several bits of said first address are interchanged based on the desired key code inputted at said key input step, to generate said second address.

ABSTRACT OF THE DISCLOSURE

Information processing method and apparatus for original image protection in a simple manner at a low cost. When data is stored, a desired key code is inputted from an operation unit. An address conversion unit converts an address from an address output unit designating a storage position of a frame memory into a physical address of the frame memory based on the input desired key code, and the data is stored into a storage area of the frame memory designated by the converted physical address. As the data stored in the frame memory is held in this manner, even if the data is read out, an original cannot be reproduced as long as address conversion algorithm is unknown. Further, before the key code inputted from the operation unit is sent to the address conversion unit, it is shuffled in a key register. Thus key code security is improved.

# FIG. 1

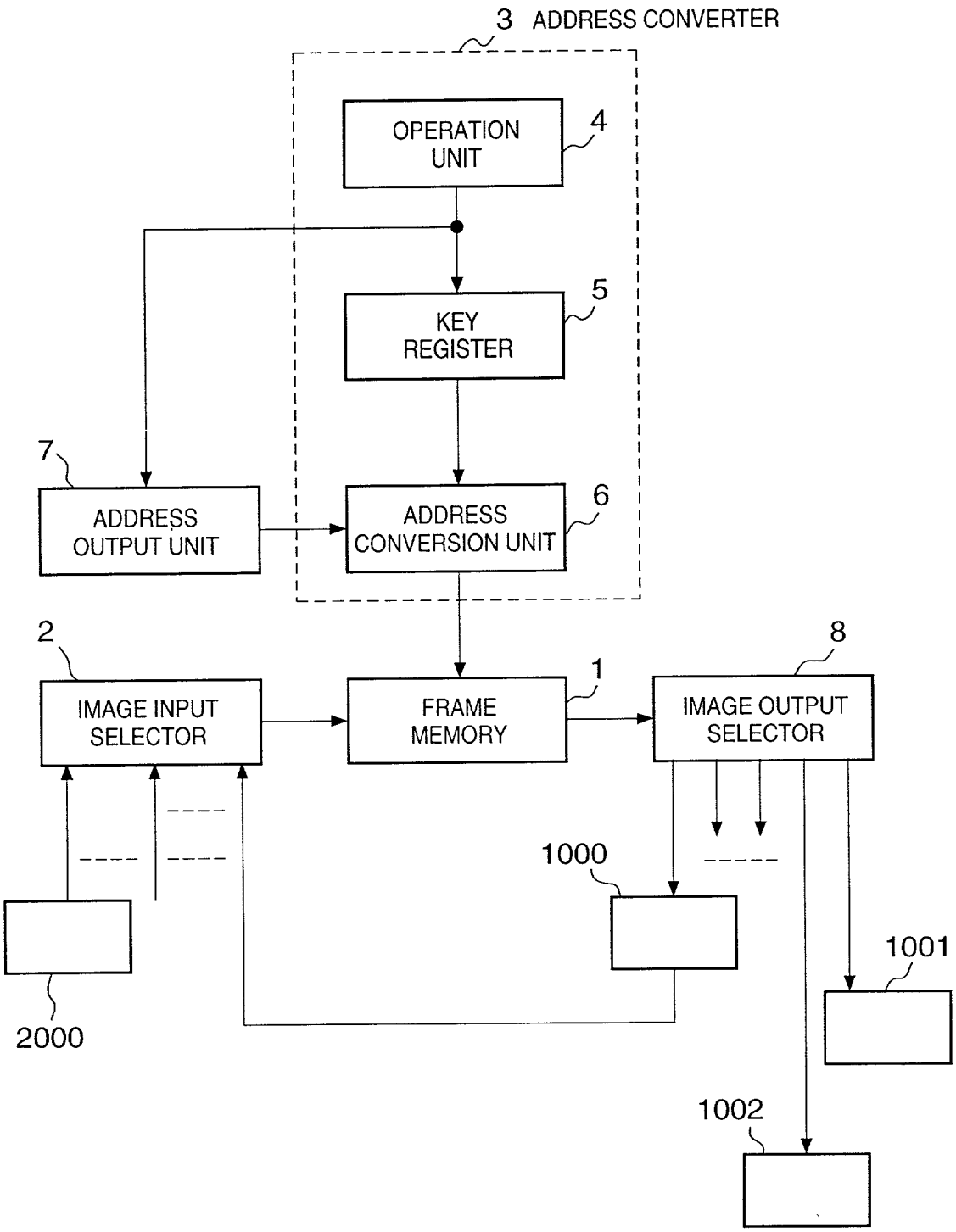

3 ADDRESS CONVERTER
OPERATION UNIT
4
KEY REGISTER
5
7
ADDRESS OUTPUT UNIT
ADDRESS CONVERSION UNIT
6
2
IMAGE INPUT SELECTOR
FRAME MEMORY
1
8
IMAGE OUTPUT SELECTOR
1000
1001
1002
2000

FIG. 2

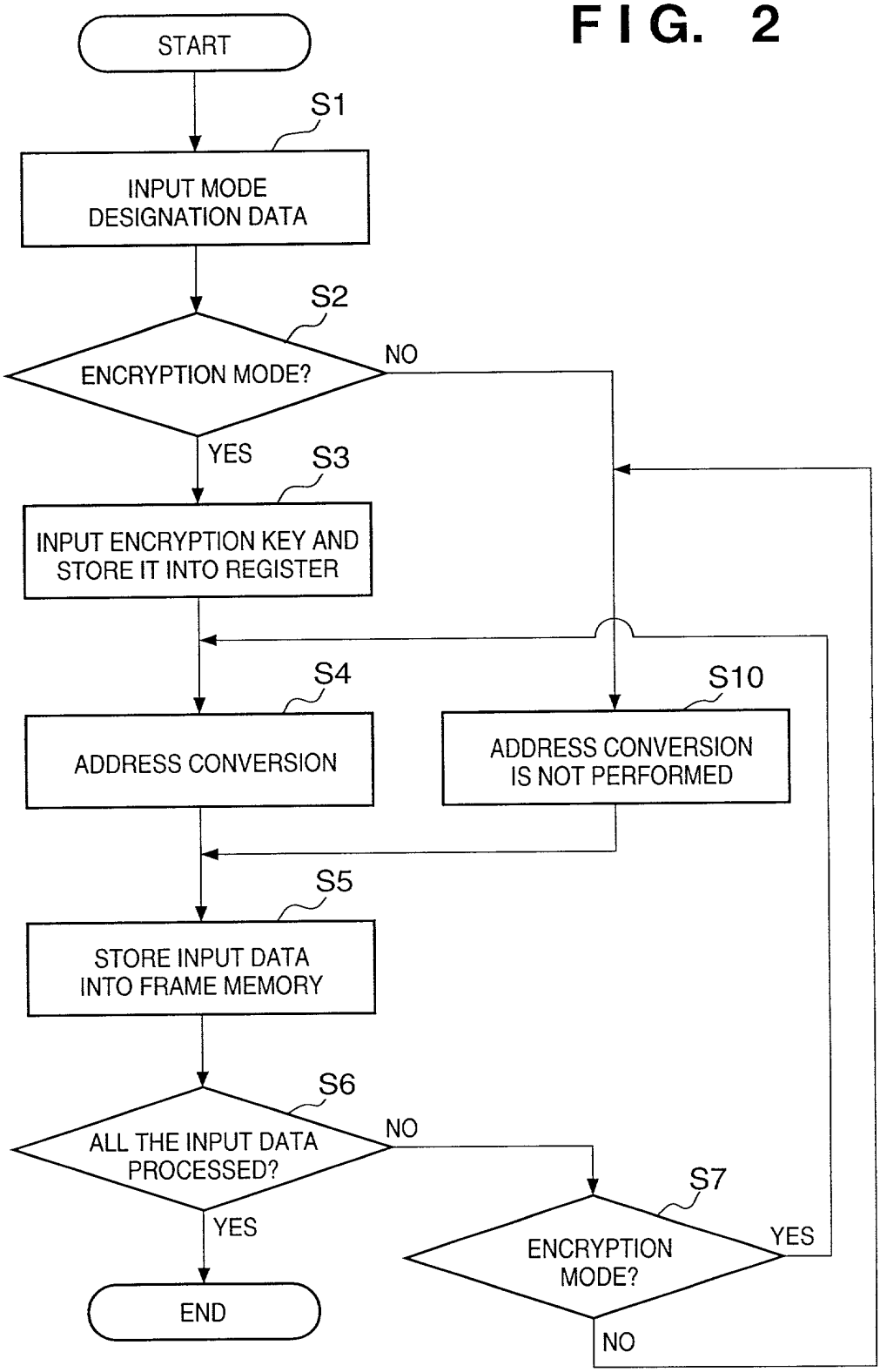

START
S1
INPUT MODE DESIGNATION DATA
S2
ENCRYPTION MODE?
NO
YES
S3
INPUT ENCRYPTION KEY AND STORE IT INTO REGISTER
S4
ADDRESS CONVERSION
S10
ADDRESS CONVERSION IS NOT PERFORMED
S5
STORE INPUT DATA INTO FRAME MEMORY
S6
ALL THE INPUT DATA PROCESSED?
NO
YES
S7
ENCRYPTION MODE?
YES
NO
END

FIG. 3

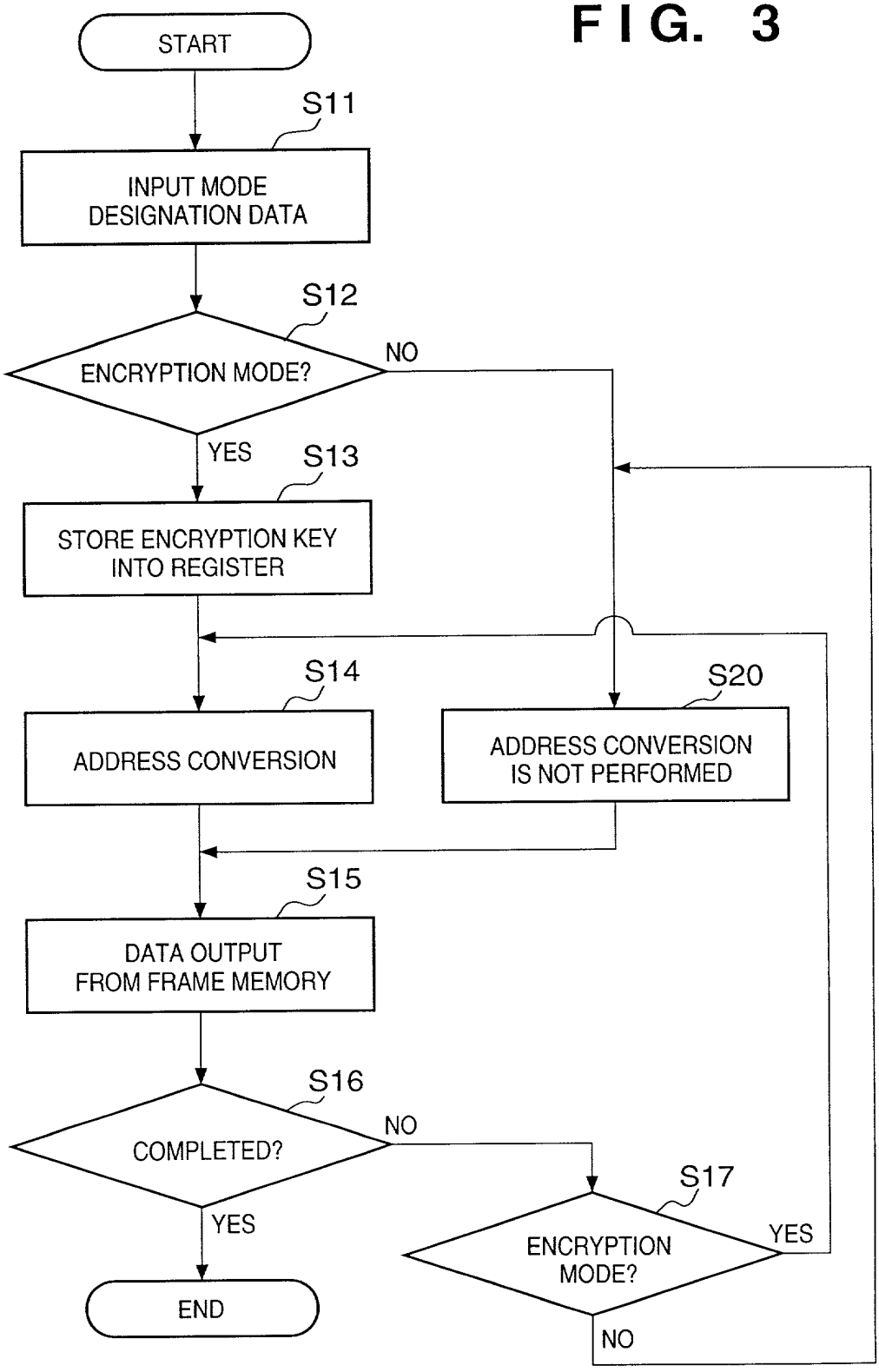
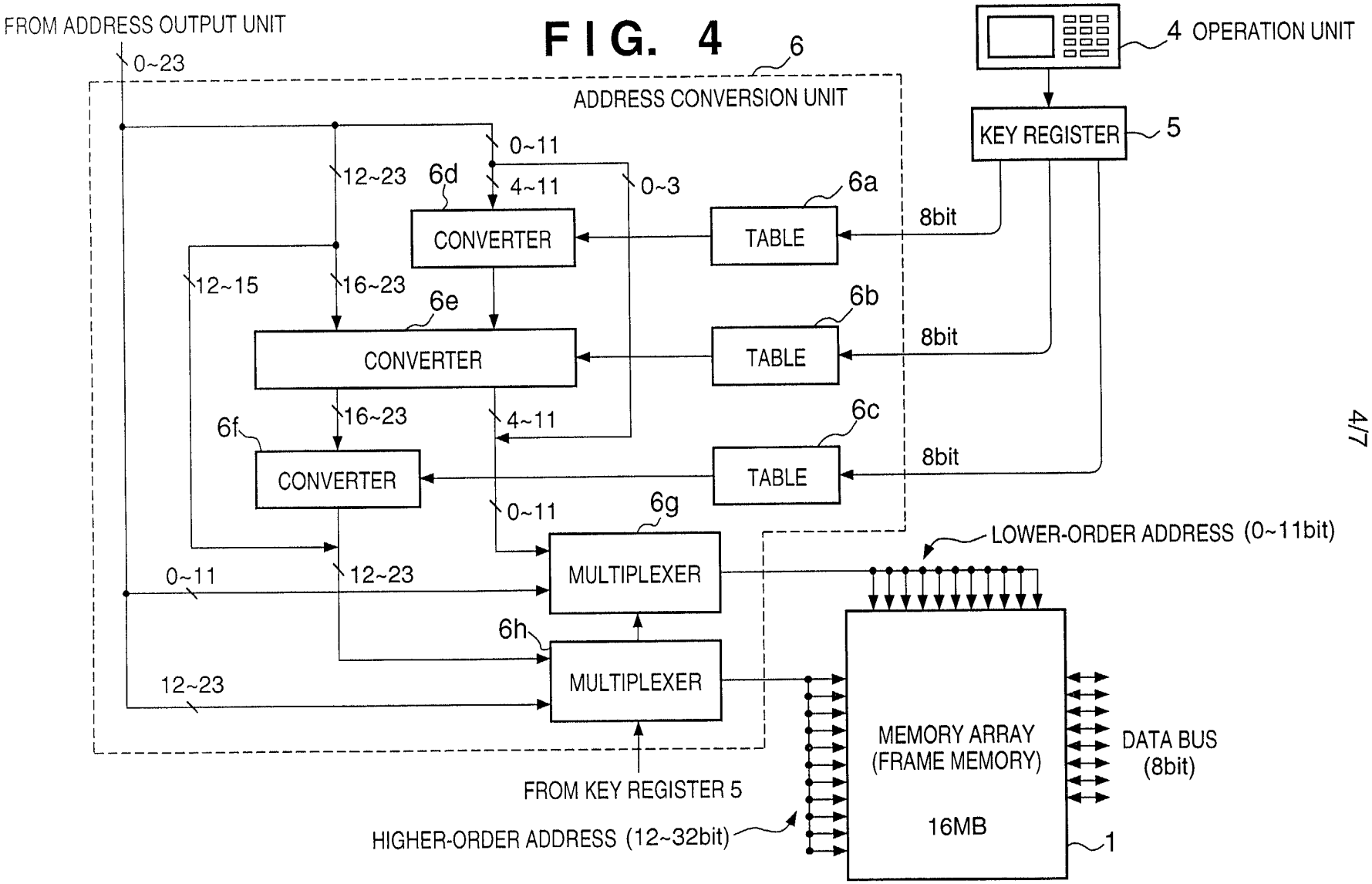

START
S11
INPUT MODE DESIGNATION DATA
S12
ENCRYPTION MODE?
NO
YES
S13
STORE ENCRYPTION KEY INTO REGISTER
S14
ADDRESS CONVERSION
S20
ADDRESS CONVERSION IS NOT PERFORMED
S15
DATA OUTPUT FROM FRAME MEMORY
S16
COMPLETED?
NO
YES
END
S17
ENCRYPTION MODE?
YES
NO

FIG. 4


FROM ADDRESS OUTPUT UNIT
0~23
6
ADDRESS CONVERSION UNIT
4 OPERATION UNIT
KEY REGISTER
5
0~11
12~23
6d
4~11
0~3
6a
CONVERTER
TABLE
8bit
12~15
16~23
6e
6b
CONVERTER
TABLE
8bit
16~23
4~11
6f
6c
CONVERTER
TABLE
8bit
0~11
6g
LOWER-ORDER ADDRESS (0~11bit)
0~11
12~23
MULTIPLEXER
6h
12~23
MULTIPLEXER
MEMORY ARRAY
(FRAME MEMORY)
16MB
DATA BUS
(8bit)
1
FROM KEY REGISTER 5
HIGHER-ORDER ADDRESS (12~32bit)

# FIG. 5

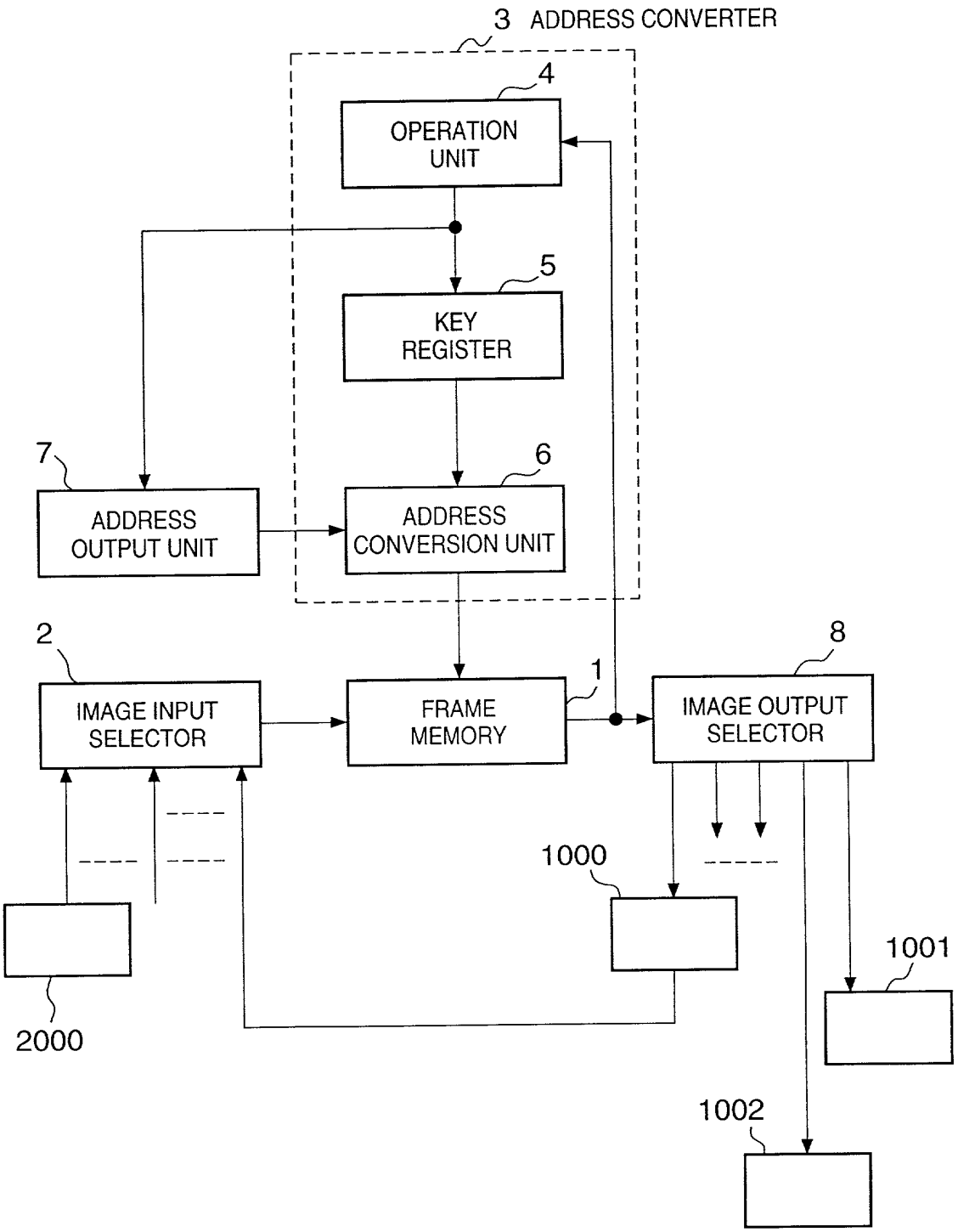

3 ADDRESS CONVERTER
4
OPERATION UNIT
5
KEY REGISTER
7
ADDRESS OUTPUT UNIT
6
ADDRESS CONVERSION UNIT
2
IMAGE INPUT SELECTOR
1
FRAME MEMORY
8
IMAGE OUTPUT SELECTOR
1000
1001
1002
2000

FIG. 6

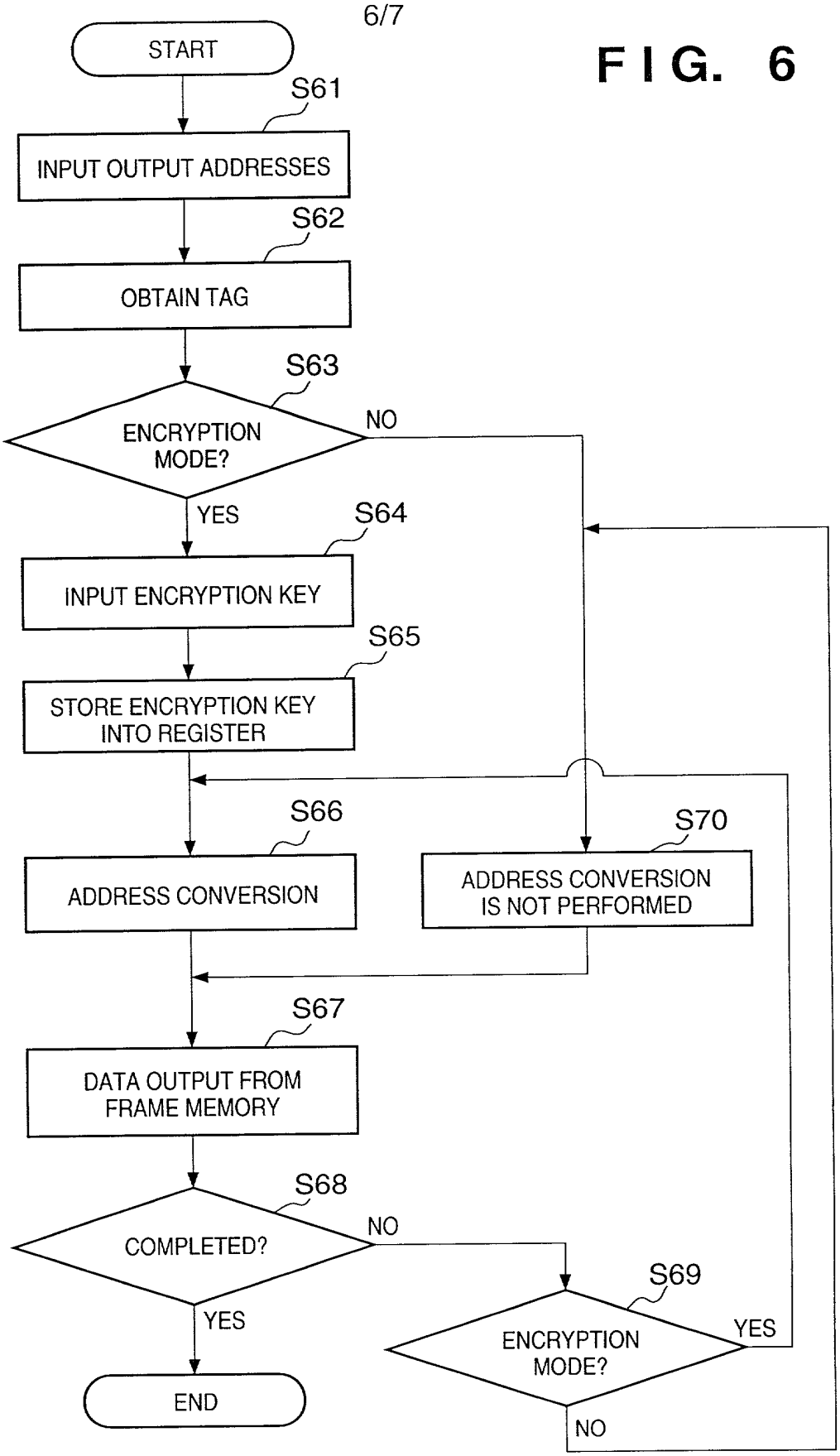
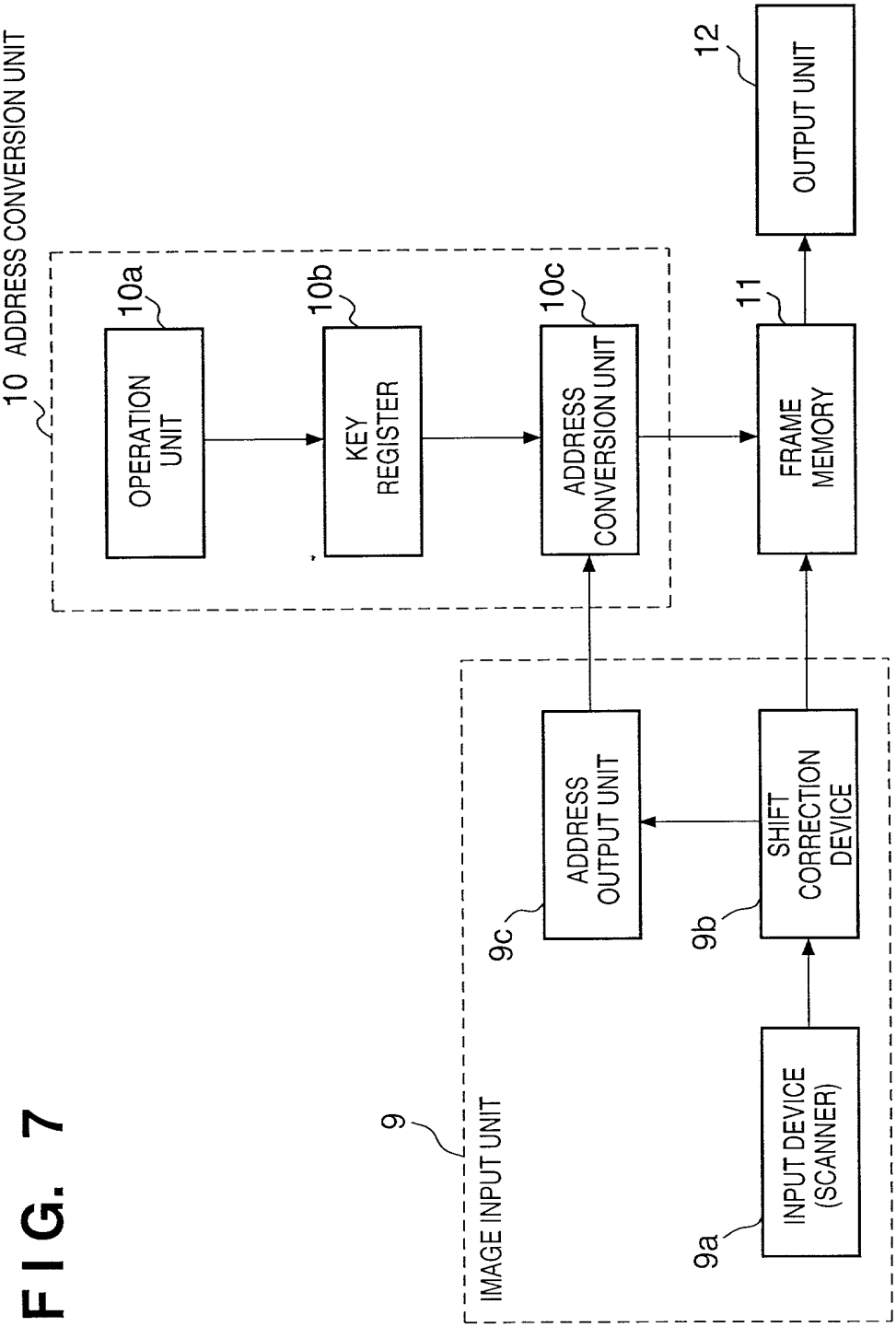

START
S61
INPUT OUTPUT ADDRESSES
S62
OBTAIN TAG
S63
ENCRYPTION MODE?
NO
YES
S64
INPUT ENCRYPTION KEY
S65
STORE ENCRYPTION KEY INTO REGISTER
S66
ADDRESS CONVERSION
S70
ADDRESS CONVERSION IS NOT PERFORMED
S67
DATA OUTPUT FROM FRAME MEMORY
S68
COMPLETED?
NO
YES
S69
ENCRYPTION MODE?
YES
NO
END

FIG. 7


10 ADDRESS CONVERSION UNIT
10a
OPERATION UNIT
10b
KEY REGISTER
10c
ADDRESS CONVERSION UNIT
11
FRAME MEMORY
12
OUTPUT UNIT
9
IMAGE INPUT UNIT
9c
ADDRESS OUTPUT UNIT
9b
SHIFT CORRECTION DEVICE
9a
INPUT DEVICE (SCANNER)

CFM 2012 US

P200-0226US

# COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

(Page 1)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

INFORMATION PROCESSING METHOD AND APPARATUS,

the specification of which [X]is attached hereto. [ ] was filed on _____ as United States Application No. or PCT International Application No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b), of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designates at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT international application having a filing date before that of the application on which priority is claimed:

| Country | Application No. | Filed (Day/Mo./Yr.) | (Yes/No) Priority Claimed |
|---|---|---|---|
| JAPAN | 11-279374 | 30/09/1999 | Yes |

I hereby appoint the practitioners associated with the firm and customer number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to the address associated with that Customer Number:

**FITZPATRICK, CELLA, HARPER & SCINTO**
**Customer Number: 05514**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor Yoshiji KANAMOTO

Inventor's signature Yoshiji Kanamoto

Date 26/09/2000 Citizen/Subject of JAPAN

Residence c/o Canon Daini Moegino Ryo, 27-6, Moegino, Aoba-ku, Yokohama-shi, Kanagawa-ken, Japan

Post Office Address c/o CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, Japan

F511/A601948/ald